Certificación electrónica con tecnologías libres: Proyecto Tibisay

Antonio Araujo Brett

13 de Noviembre de 2015

Proyecto Tibisay

Desarrollar un conjunto de herramientas informáticas con tecnologías libres que permitan el uso y masificación de la certificación electrónica en actividades de gobierno electrónico para la República Bolivariana de Venezuela

Proyecto Tibisay

Formato de documento firmado electrónicamente

BDOC: basado en XAdES y con origen en Europa del Este

Estructura de un archivo BDOC

BDOC: basado en XAdES y con origen en Europa del Este

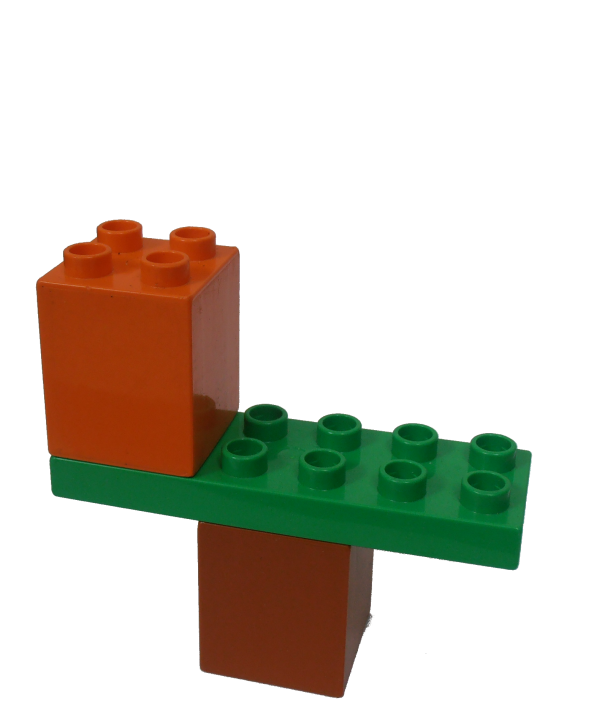
Estructura de un archivo BDOC

Bibliotecas de desarrollo

Bibliotecas de desarrollo

- Libdigidocpp: C++.
- JDigiDoc, digidoc4j: Java.
- Libfirmaxml: C++.
- Envoltorio Python para Libsafet (flujo de trabajos y firmas electrónicas en C++).

Aplicación de escritorio



Tibisay Firma XML

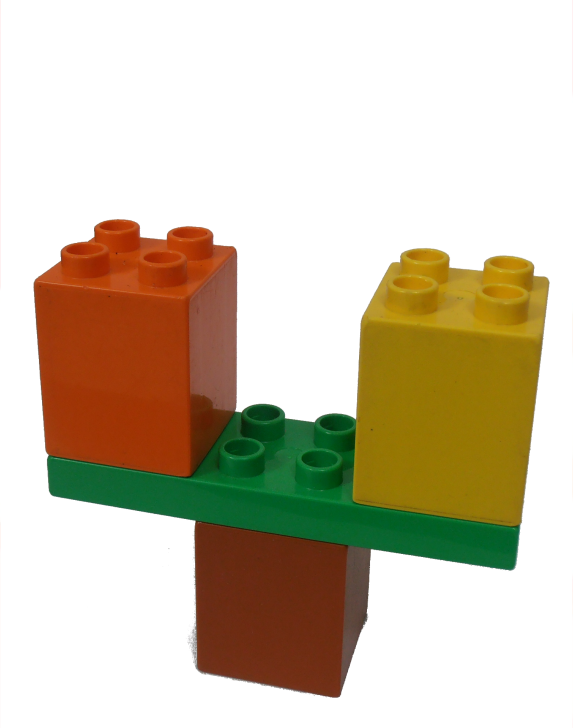
- Aplicación de escritorio para firmar electrónicamente y verificar firmas, cifrar y descifrar documentos.
- Desarrollada en C++ con el framework Qt, QML y la biblioteca Libdigidocpp.
- Licencia GPL 2.
- *http://tibisay.cenditel.gob.ve*.

¿Qué se puede firmar?


Tibisay
Gobierno Bolivariano de Venezuela
Ministerio del Poder Popular para Ciencia, Tecnología e Innovación
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)
Tibisay Firma XML
Firmar
Verificar
Cifrar
Descifrar
Tibisay Firma XML


FUNDACIÓN INSTITUTO DE INGENIERÍA
PSC
Proveedor de Servicios de Certificación
Electrónica del Estado Venezolano

Aplicación móvil



Tibisay Móvil

Aplicación móvil para firmas electrónicas y cifrado con certificados electrónicos en software libre.

Android versiones: 2.3.3 y superior.
Código reutilizado de aplicación MobileSign desarrollada por SUSCERTE.

CENDITEL

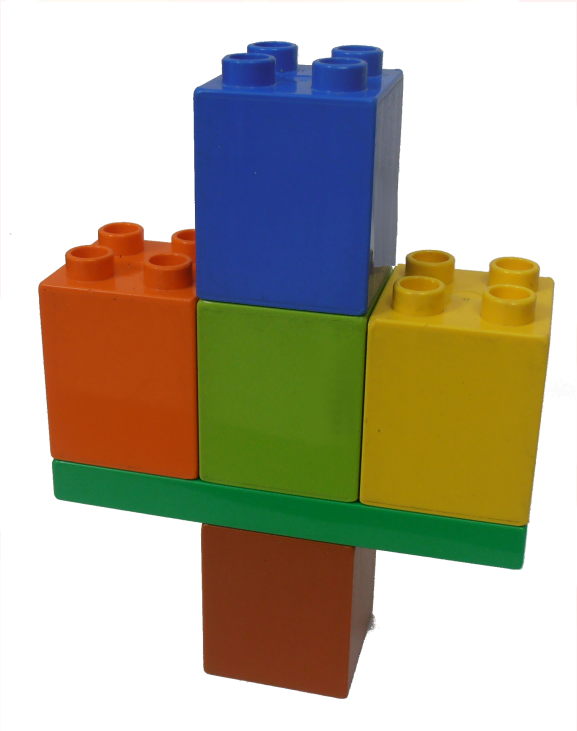
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)

Servicio web

Murachí: Servicio web de firma y verificación de documentos

- https://tibisay.cenditel.gob.ve/murachi
- API REST.
- Firma electrónica y verificación de documentos en formato PDF y BDOC.
- Uso de componente para firma electrónica desde navagedor web con soporte para dispositivo criptográfico.
- Licencia AGPL.

Portal de verificación



Portal de verificación y firma electrónica - Mozilla Firefox

https://murachi.cenditel.gob.ve/pruebaservicioweb/

CENDITEL | Home | Wiki | Contacto

Portal de firma electrónica y verificación

Sistema para firmar electrónicamente documentos y verificar los documentos firmados

Firmar | Verificar

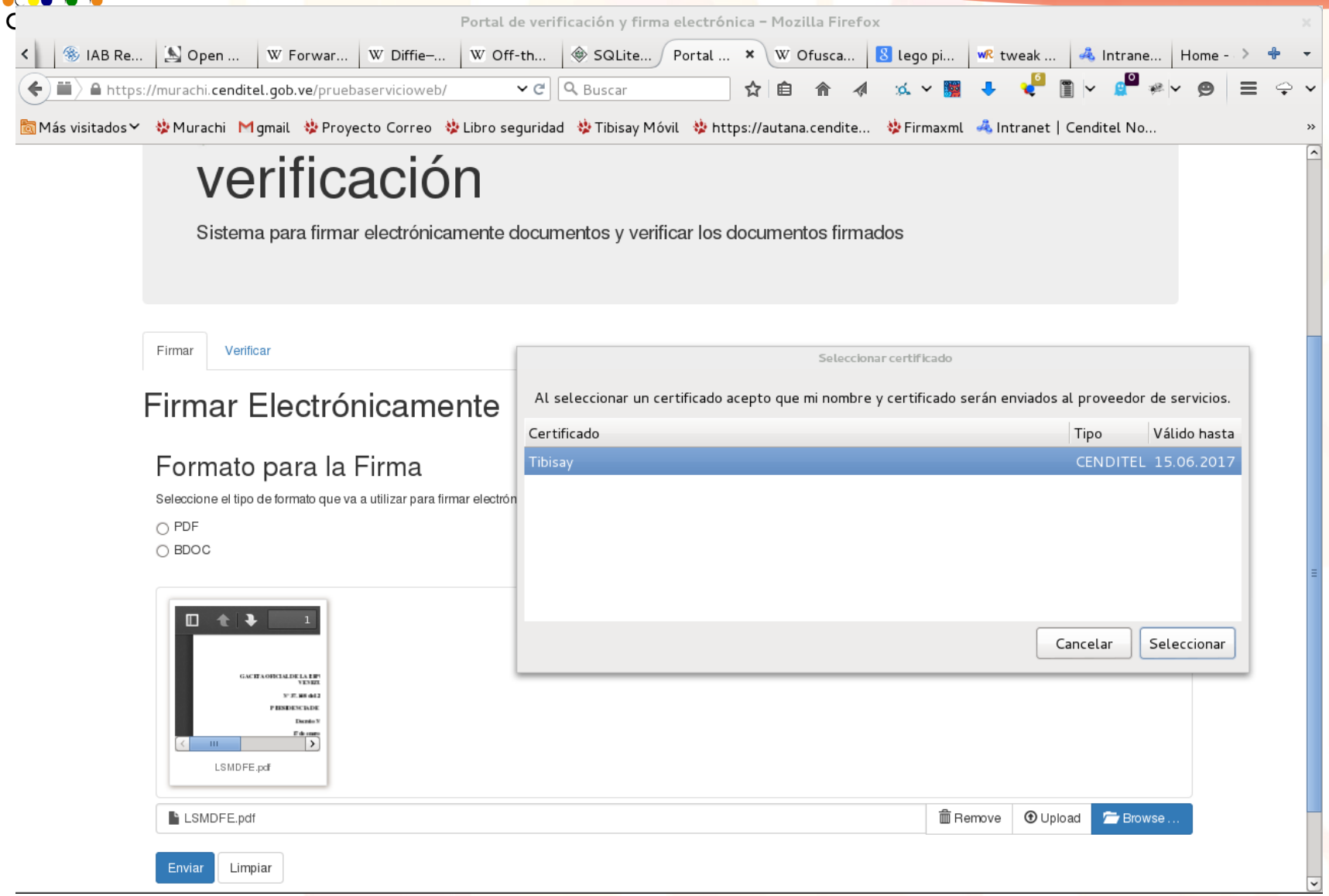
Firmar Electrónicamente

Formato para la Firma

Seleccione el tipo de formato que va a utilizar para firmar electrónicamente

- PDF
- BDOC

Browse ...


Portal de verificación y firma electrónica - Mozilla Firefox
https://murachi.cenditel.gob.ve/pruebaservicioweb/
verificación
Sistema para firmar electrónicamente documentos y verificar los documentos firmados
Firmar
Verificar
Firmar Electrónicamente
Formato para la Firma
Seleccione el tipo de formato que va a utilizar para firmar electrón
PDF
BDOC
Seleccionar certificado
Al seleccionar un certificado acepto que mi nombre y certificado serán enviados al proveedor de servicios.
Certificado
Tipo
Válido hasta
Tibisay
CENDITEL
15.06.2017
Cancelar
Seleccionar
LSMDFE.pdf
Remove
Upload
Browse ...
Enviar
Limpiar

Portal de verificación y firma electrónica - Mozilla Firefox

https://murachi.cenditel.gob.ve/pruebaservicioweb/

Información de la firma electronica

Número de firmas existentes en el archivo: 2

Información de la firma: 1

10 records per page

Search:

#	Campo	Descripción
1	Tipo de firma de archivo PDF	approval
2	Fecha en que se realiza la firma	10-04-2015 15:37:39.00
3	Chequea la integridad de la firma	true
4	Estampilla de tiempo	null
5	Razón de la firma	Aprobación
6	Ubicación donde se realiza la firma	Caracas
7	Nombre alternativo del firmante	Jose Joaquin Contreras Garcia
8	Fecha de inicio de validez del certificado	2015-03-31 08:42:30.00
9	El certificado todavía está válido	true
10	La firma abarca todo el documento PDF	false

Showing 1 to 10 of 24 entries

Previous 1 2 3 Next

CENDITEL

Proyecto Tibisay

Proyecto Murachí

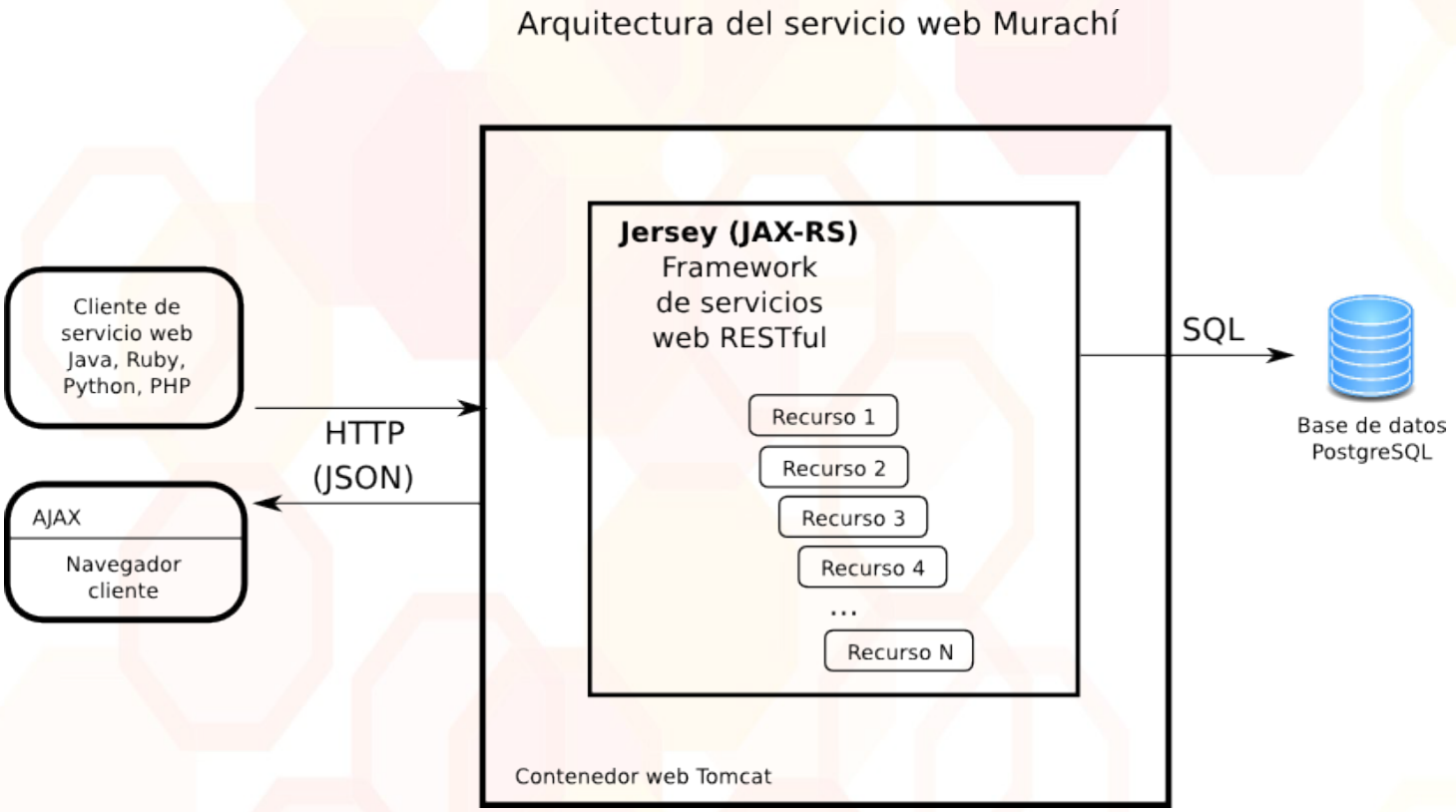
Murachí: Plataforma de desarrollo

- Sistema operativo Debian GNU/Linux Wheezy.
- Java
- IDE Eclipse Luna.
- Jersey. Implementación para Java API for RESTful Web service.
- Maven: herramienta de administración de proyectos de software.
- Tomcat: software que implementa contenedores web.
- Biblioteca iText para gestión de archivos en formato PDF.
- Biblioteca digidoc4j biblioteca para integrar firmas electrónicas basadas en XAdES.

Murachí: Plataforma de operación

- Sistema operativo Debian GNU/Linux
- Java 1.7
- Tomcat 7

Murachí: arquitectura



Estilo arquitectónico REST.

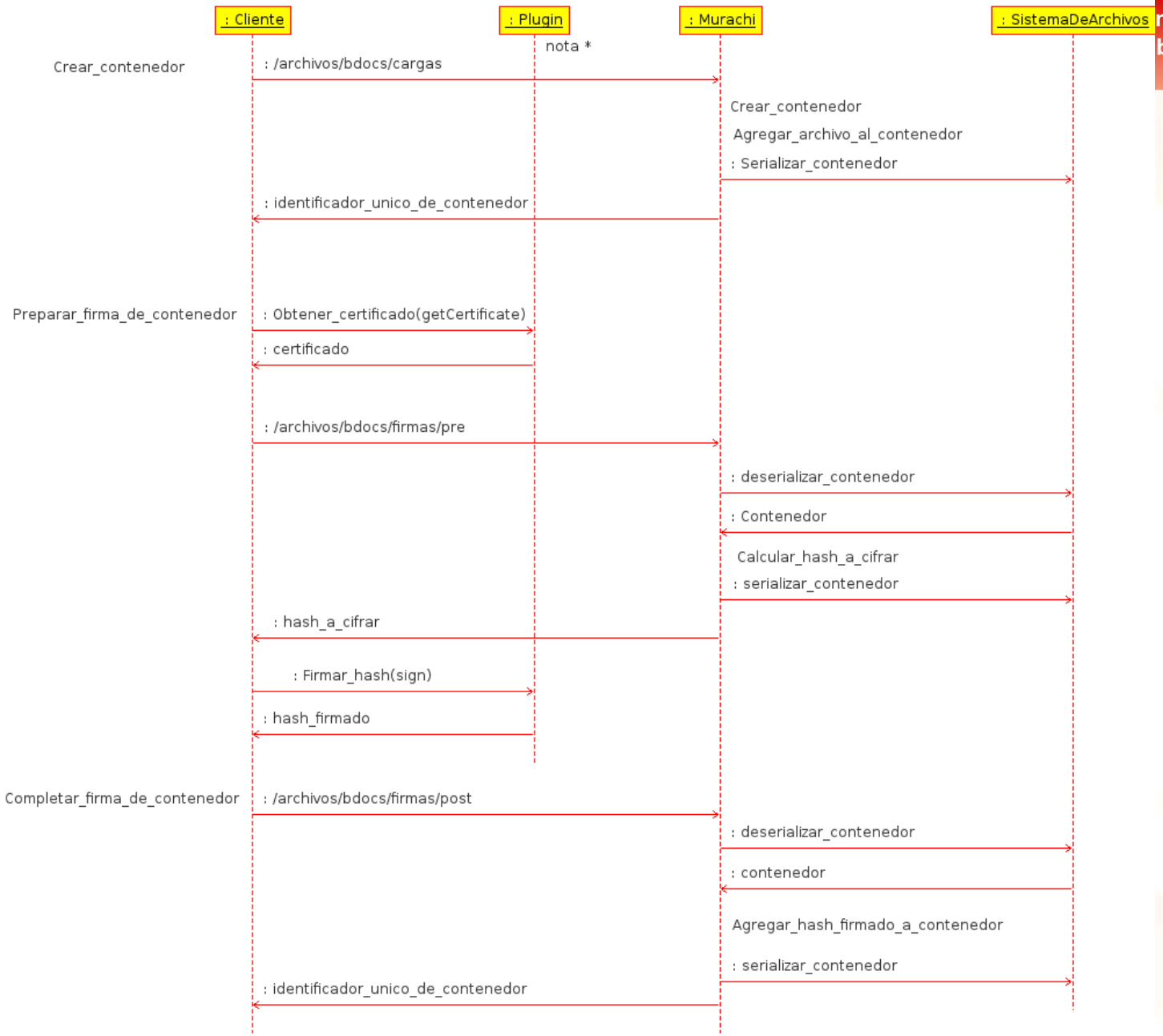
Murachí: complemento de navegador web

- Firma electrónica con dispositivo criptográfico: token USB o tarjeta inteligente.
- Complemento (plugin) *esteidfirefoxplugin* para navegador Mozilla y derivados *https://github.com/open-eid/browser-token-signing*.
- Obtiene el certificado electrónico del dispositivo.
- Cifra la reseña (hash) del archivo a cifrar.

Se utiliza en conjunto con la interfaz JavaScript *hwcrypto* para firmar con dispositivos criptográficos: : *https://github.com/open-eid/hwcrypto.js*.

Murachí: complemento de navegador web

Diagrama de secuencia del proceso de firma de un contenedor



*se usa biblioteca JavaScript hwcrypto para comunicarse con el plugin

Murachí: documentación de API

https://murachi.cenditel.gob.ve/apidoc/index.html

- Archivos: gestión de archivos que incluye carga, descarga y verificación de firma.
- BDOC: Preparación y completación de la firma de un documento en formato BDOC.
- General: información general del API como versión y estadísticas básicas.
- PDF: Preparación y completación de la firma de un documento en formato PDF.

Murachi: documentación de API

API Murachi - Mozilla Firefox

https://murachi.cenditel.gob.ve/apidoc/index.html

ARCHIVOS

- Carga un archivo y verifica
- Carga un archivo
- Descarga un archivo
- Verifica un archivo

BDOCS

- Agrega archivo a contenedor.
- Completa la firma de un contenedor BDOC.
- Completa la firma del archivo en formato BDOC.
- Crea un contenedor BDOC.
- Descarga un archivo del contenedor.
- Elimina un archivo del contenedor.
- Elimina una firma de un contenedor.
- Lista de archivos del contenedor.
- Lista de firmas de un contenedor.
- Número de archivos de contenedor.
- Número de firmas de un contenedor.
- Prepara la firma de un archivo en formato BDOC.
- Prepara la firma de un contenedor BDOC.

GENERAL

- Retorna estadísticas básicas de

Murachi

0.1.0

API para verificación y firma electrónica de archivos PDF y BDOC

Archivos

Archivos - Carga un archivo y verifica

0.1.0

Carga un archivo a través de un formulario y retorna un json con la información de la firma.

POST

```
https://murachi.cenditel.gob.ve/Murachi/0.1/archivos/firmados
```

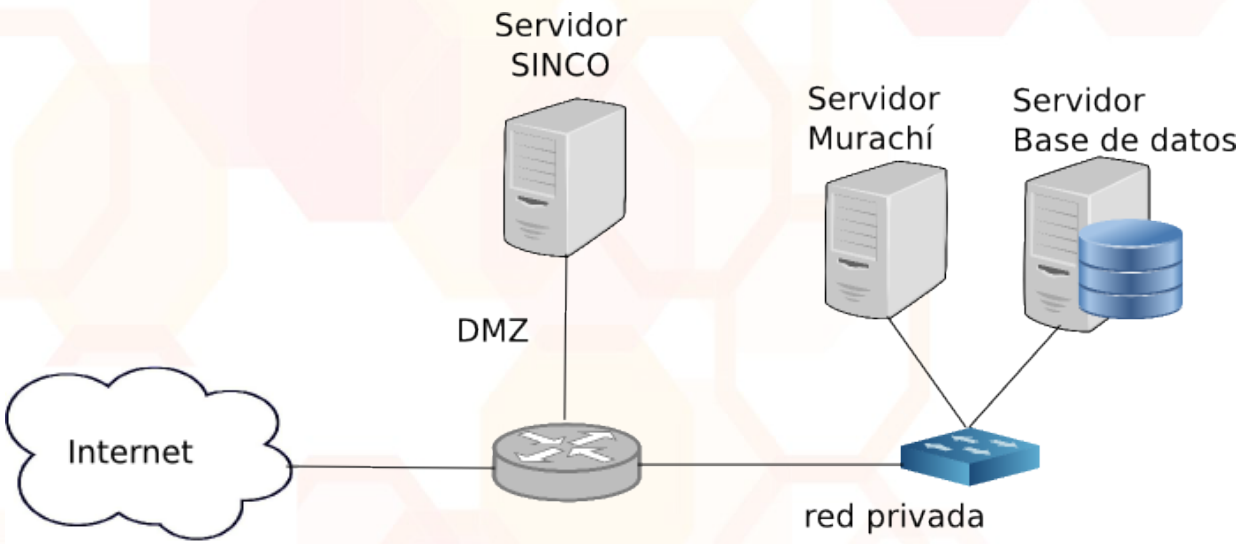
Example usage:

```
var formData = new FormData();
formData.append("upload", $("#file-sign")[0].files[0]);
$.ajax({
        url: "https://murachi.cenditel.gob.ve/Murachi/0.1/archivos/firmados",
        type: "post",
        dataType: "json",
        data: formData,
        cache: false,
        contentType: false,
        processData: false,
        headers: {"Authorization":"Basic YWRtaW46YWRtaW4="},
        success: function(response) {
                var json = JSON.stringify(response);
                alert(json);
        },
        error: function(response){
```

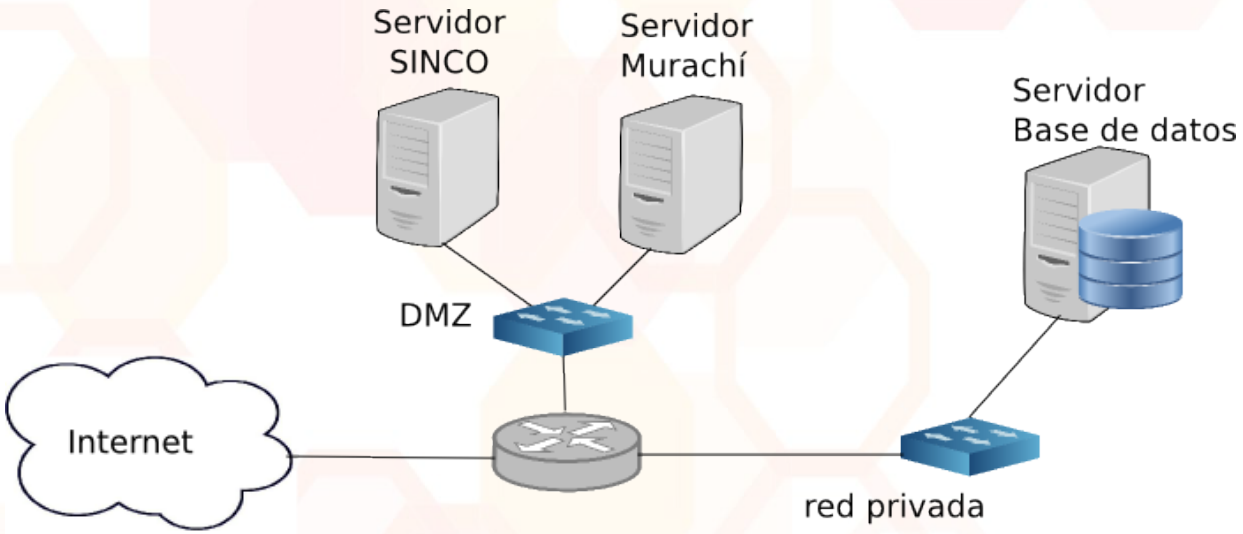
¿Cómo usar el API de Murachí?

https://tibisay.cenditel.gob.ve/murachi/wiki/comoUsarElApi

Despliegue de Murachí: red privada



Despliegue de Murachí: red pública



Equipo de trabajo

- Antonio Araujo (aaraujo@cenditel.gob.ve),
- Pedro Buitrago (pbuitrago@cenditel.gob.ve),
- Víctor Bravo (vbravo@cenditel.gob.ve),
- Erwin Paredes (eparedes@cenditel.gob.ve),
- Jorge Redondo (jredondo@cenditel.gob.ve)

¿Y por qué Tibisay?, ¿Y Murachí?

https://tibisay.cenditel.gob.ve/trac/wiki/origenNombre

Contacto

https://tibisay.cenditel.gob.ve/murachi

seguridad@cenditel.gob.ve